Job Description:

The Chief Information Security Officer (CISO) reports to the Chief Information Officer of the Office for Information Resources and is responsible for maintaining and advancing the State's enterprise-wide information security management program to ensure that information assets and critical infrastructure are adequately protected. This position is also responsible for identifying, evaluating and reporting on information security risks in a manner that meets the State's legal, regulatory and contractual requirements.

The CISO proactively and collaboratively works with departments, agencies and boards, of the State, to develop and implement policies and procedures that meet defined standards for information security management.

The ideal candidate is an integrator of people and processes, an innovative leader, a problem solver, an effective consultant, and possesses solid domain competency in the field of information security management by having demonstrated experience in a leadership role.

Responsibilities:

- Assess the current security program, including policies, procedures, and organization and make recommendations for improvement.
- Develop business-relevant metrics to measure the efficiency and effectiveness of the State's information security management program, facilitate appropriate resource allocation and increase the maturity of the program.
- Ensure the information security management program supports compliance with applicable laws, regulations, contractual requirements, and policies (e.g., the Health Insurance Portability and Availability Act, the Payment Card Industry Data Security Standard and the Internal Revenue Service Tax information Security Guidelines) to minimize or eliminate risk and address audit findings.
- Develop a threat intelligence strategy and incorporate threat intelligence into the security program.
- Maintain a program of regularly scheduled security audits and assessments to evaluate policy compliance and existing defenses and to identify vulnerabilities.
- Provide subject matter expertise to executive management on a broad range of information security standards and best practices (e.g. the ISO/IEC 27000 series, the NIST Computer Security Division Special Publications and Federal Information Processing Standards, the Payment Card Industry Data Security Standard) and offer strategic and tactical security guidance for all IT projects, including the evaluation and recommendation of technical controls.
- Work with OIR senior management and directors to ensure appropriate technologies are in place to safeguard the State of Tennessee's infrastructure and data assets.
- Oversee and enhance the existing security awareness program.
- Work directly with State departments, agencies and boards to (i) establish and facilitate IT risk assessment and risk management processes, including the reporting and oversight of

remediation efforts to address negative findings; (ii) identify acceptable levels of risk; and (iii) establish roles and responsibilities with regard to information classification and protection. With the IT-ABC, consult with State departments and agencies on potential systems purchases and implementations to ensure that information security concerns are understood and addressed holistically.

- Oversee incident response planning and management of security incidents and events to protect State IT assets (e.g. information, critical infrastructure, intellectual property, and reputation), such duties to include overseeing the investigation of security breaches and assisting with disciplinary and legal matters associated with such breaches, as necessary.
- Oversee Coordinate the use of external resources involved in the information security management program, including, but not limited to, interviewing, assisting in negotiating contracts and fees and managing external resources.
- Oversee vulnerability management, including, but not limited to maintaining a centralized scanning environment, identifying scan targets (hardware and web applications), listing and scheduling scans, and working with target owners to remediate identified vulnerabilities.
- Oversee disaster recovery program, including, but not limited to auditing and testing OIR recovery plans, promoting the importance of disaster recovery and continuity planning to agencies, and the performance of business impact analyses.
- Work with the State's CIO to coordinate and manage public relations activities as they relate to the information security program and incident response.
- Maintain relationships with local, state and federal law enforcement and other related government agencies.

Minimum Requirements:

- Bachelor’s degree in business administration or a technology related field, or 10 years experience in an information technology role, five of which are in information security or risk management.
- Professional certification such as CISSP, CISA or CISM
- Valid Class D Driver's License
- US Citizen
- Candidate must be able to receive a pass status from a TBI background check.
- Candidate must be able to receive a Federal Secret Security Clearance.

Preferred Knowledge/Abilities/Experience:

- Excellent written and verbal communication skills, interpersonal and collaborative skills, and the ability to communicate security and risk-related concepts to technical and non-technical audiences.
- Must be a critical thinker with strong problem-solving skills.
- Up-to-date knowledge of technological trends and developments in the area of information security, governance, risk and compliance management, and data loss prevention.

- Knowledge of information security standards, codes of practice and guidelines such as the ISO/IEC 27000 series, the NIST Computer Security Division Special Publications and Federal Information Processing Standards, and the Payment Card Industry Data Security Standard.
- Project management skills, including financial/budget management, scheduling and resource management, certification as PMP or related certification a plus
- Ability to lead and motivate cross-functional, interdisciplinary teams to achieve tactical and strategic goals.
- Experience working with C level executives.
- Experience in budgeting to provide for security technologies, controls and training.
- High level of personal integrity, and the ability to professionally handle confidential matters and exhibit the appropriate level of judgment and maturity.
- High degree of initiative, dependability and ability to work with little supervision.